Remembering and forgetting in the digital age – a position paper

Thouvenin, Florent ; Burkert, Herbert ; Hettich, Peter ; Harasgama, Rehana

informationresearch

VOL. 21 NO. 1, MARCH, 2016

---

eRemembrance or eOblivion? International Conference on Society's Memory Functions in the Digital World, University of Tampere, Finland, Tampere 23-24 November, 2015

Remembering and forgetting in the digital age – a position paper

Florent Thouvenin, Herbert Burkert, Peter Hettich and Rehana Harasgama

Abstract

Introduction. The paper introduces a framework that provides guidelines for legislators and private or public organisations on how to make decisions on remembering and forgetting (personally identifiable) information in the information society.
Method, analysis and results. The paper is the result of a comprehensive analysis of the current legal framework for remembering and forgetting personally identifiable information and two interdisciplinary workshops. It proposes a simple framework that consists of two blocks: (1) alternative mechanisms that can be applied instead of deleting information, i.e. access restrictions, use restrictions and the transfer of data; and (2) a set of criteria that must be considered when taking this decision, i.e. the relevance, the impact and the redundancy of information as well as the efficacy of deleting information.
Conclusions. The paper reflects the insight that the complexity of information handling, the unpredictability of possible future uses of information, the fast technological development and the unforeseeable impact of technology on the behaviour of individuals, governments and organisations all call for a precautionary approach when dealing with remembering and forgetting. Accordingly, the paper advocates for favouring remembering over forgetting and applying alternative mechanisms such as access and use restrictions instead of simply deleting information.

Introduction

For the past three years, the authors of this paper have been working on a research project on *Remembering and forgetting in the digital age*. The research was conducted in close collaboration with an international network of researchers from various disciplines such as psychology, philosophy, economics, IT, sociology and history. The research project analyses if and in what way the current legal framework – under interdisciplinary considerations – and other normative aspects can provide adequate solutions for handling (personally identifiable) information. The ultimate goal of the research project is to create a design guide that provides guidelines on how to best handle (personally identifiable) information in a legal framework. This design guide is presented in this paper.

Counterbalancing the default switch

Advances in information technology, namely storing and software technologies, suggest that it has become technically feasible and economically viable to design information systems that build on storage as a default rule rather than implement procedures for information exclusion and destruction (see Minutes: http://rememberingandforgetting.wikispaces.com/Research). At the same time, it has been pointed out that these advances have created new risks for individuals, groups and organisations by binding them to their past and reducing their opportunities to adapt to change or innovate. Procedures, it has been argued, need to be implemented that counterbalance what we call *remembering trends* with intentional deletion operations and emphasise precautionary approaches such as minimising the accumulation of information when designing information systems (Mayer-Schönberger, 2009).

Against this background, the starting point of the research that ultimately led to this paper was the preliminary assumption that the digitalisation of information has triggered a default switch of fundamental significance. Forgetting information was the default in the analogous age and remembering only took place because of deliberate decisions. Today, digital information is remembered by default and it is only forgotten if someone deliberately decides to delete it. In the course of the research, this preliminary assumption roughly proved to be true although certain aspects need to be specified.

First, remembering and forgetting information needs to be distinguished from the mere storage and deletion of data. Whereas storing and deleting only relate to the – often fully automated – technical process of retaining or disposing data, remembering and forgetting involve more than that. Today, remembering usually involves human interaction with the information, such as consultation, organisation or use. To this extent, remembering is a much more deliberate and intellectual process as it encompasses structuring, connecting and curating information. However, in the near future, machines could possibly carry out even these forms of interaction. Hence, the scope of the default switch is less fundamental than it appears at first sight, since the new default is in fact not remembering information but only the storing of data. What remains unchanged, however, is that remembering information will always depend on storing data while deleting data will lead to forgetting the information enshrined in such data. From this perspective, the default switch from deletion to storage only (but still) enables a default switch from forgetting to remembering.

Secondly and somewhat opposed to the preliminary assumption, preserving information in a digital environment is a much more active process than it was in the analogous world (for digital curation and digital preservation see Harvey, 2010; Digital Curation Center: Curation Lifecycle Model on http://www.dcc.ac.uk/resources/curation-lifecycle-model). This means that decisions on remembering and forgetting have to be taken both constantly and consciously. Contrary to the preliminary assumption, the state of technology as such does not per se lead to remembering as the default rule. Rather, the complexity and constant development of technology requires conscious decisions at the design stage on how to organise and implement remembering at a technological level and/or the constant migration of information from one technological environment to the next environment. This necessity arises from the technological dynamics that in the end do not guarantee by themselves retrospective compatibility. Archival institutions all over the world have made these experiences with new information technologies: since storage technologies themselves are subject to constant change, it is no longer sufficient simply to store the data. Rather, it is necessary to store the means that secure the readability of such data over time as well. Therefore, the default switch with regard to remembering is not guaranteed per se through technology but has to be ensured politically at every instance bearing in mind all resource allocation consequences. Data maintenance as the technical component of information storage, thus, continues to require human resources, energy and space. Insofar, technology has not solved the problem of remembering and forgetting but has added an additional layer of complexity. With the need for conscious design decisions and constant migration of data in mind, the preliminary assumption only holds under the condition that such decisions are taken and the necessary steps for the constant migration of data are actually carried out.

Thirdly, at least from today's perspective, it seems fair to assume that the constant migration of data has become the default since the cost of deciding what data should be retained and what data disposed of is usually greater than the cost of migrating and storing data in a current format and on current devices.

Fourthly, the legal system has already reacted to a certain extent and has provided possible answers to the default switch. Namely, the European Court of Justice has acknowledged a *right to be forgotten* according to which individuals have the right – under certain conditions – to ask search engines to remove links with personal information about them from their displayed search results (Google Spain SL et al. vs. Mario Costeja Gonzalez et al., 2014). In addition, the European Court of Justice has declared invalid the Data Retention Directive (European Union, 2002), which had required the providers of publicly available

electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities (Digital Rights Ireland Ltd vs. Minister for Communications, Marine and National Resources et al., 2014).

Addressee, aim and scope

This position paper introduces a design guide that is addressed to all those responsible for setting rules related to the handling of information such as international, national or regional regulators and those responsible for setting the rules for information management in public and private organisations. In addition, the process proposed in this design guide can be applied directly by those responsible for the information management in private organisations, without having to implement specific information management rules. This however, requires them to be granted a sufficient degree of discretion to make these decisions when applying the process.

The suggestions contained in this design guide build on the analysis of the current legal framework for remembering and forgetting (see Matrix) and the insights gained from the various and very rich interdisciplinary discussions conducted during the research that ultimately lead to this paper (see Minutes). These suggestions are intended to *supplement other information-handling* guides that may emphasise privacy and openness concerns and obligations, as well as record keeping duties (Beglinger, Burgwinkel, Lehmann, Neuenschwander and Wildhaber, 2008; Wildhaber *et al.*, 2015). In their substance, these suggestions may be quite similar to traditional appraisal processes used in public organizations and national archives. In scope, however, they differ fundamentally from these processes since they are addressed to international, national and regional regulators and private and public organizations alike. In other words, national archives and similar institutions follow a rationale which stems from and is limited to their mission (namely archiving, etc.); this results in an inbuilt tendency towards remembering, which this design guide tries to overcome by offering a holistic perspective. As opposed to other general information-handling guides, this design guide can be seen as a reaction to the trend in recent privacy literature that emphasises the importance of forgetting in a digital environment. From this perspective, the suggestions contained in this design guide try to complement other existing guides and aim at enabling more balanced and better-reflected reactions to the challenges of the (perceived) dangers of ubiquity and longevity of digital data.

This design guide is not limited to the handling of *personally identifiable information* but addresses the handling of information as such. This does not alter the fact that special attention needs to be given to personally identifiable information because of its close connection to core values of the legal system. However, the design guide acknowledges the experience that the defining lines between personally identifiable and not personally identifiable information are increasingly difficult to draw in an environment shaped by very large information collections and increasingly sophisticated analytical tools (Schwartz and Solove, 2011). Consequently, this design guide refrains from trying to draw a line between (seemingly) different categories of data.

Furthermore, this design guide does not aim at establishing a new legal order for data protection law. Rather, it restricts itself to establishing a framework that consists of possible alternatives to the irreversible act of deleting information and a set of criteria that should be considered when making a decision on remembering or forgetting specific information. As a matter of course, the application of this framework does not discharge individuals, organisations and governments from complying with the requirements of existing *data protection law*. However, the suggestions contained in this design guide may advocate for a different assessment and balancing of interests when applying established concepts of this body of law.

Consequences

Precautionary Approach

The suggestions contained in this design guide reflect the fundamental insight gained during the research that the complexity of the problem, the unpredictability of possible future uses of information, the fast technological development and the unforeseeable impact of technology on the behaviour of individuals, governments and organisations all call for a precautionary approach (Sunstein, 2005).

In addition to complexity and unpredictability, a more fundamental reasoning calls for a precautionary approach as well. Making decisions on remembering and forgetting at a given moment not only determines what information may be technically available for individual and social use in the future but – more importantly – it determines what kind of decisions future generations will be able to make about their future. In view of other technological developments with long term impacts that exceed the expectation horizon of one, two or even several generations, our societies and legal systems have responded by gradually acknowledging responsibility for future generations as a leading moral and legal obligation and by refraining as much as possible from setting irreversible conditions. In this respect, parallels can be drawn to other areas of law such as environmental law and the law on the protection of historic buildings and monuments. Since we are unable to assess the future impact of pollution and the future relevance of historic buildings and monuments, we should act consciously when taking irreversible decisions, i.e. staying on the safe side when allowing pollution or rather preserving than destroying historic sites when in doubt.

In our opinion, the acknowledgement of a responsibility for future generations needs to be extended to the ways we handle information in our society and to how we make decisions on what to keep and what to let go. Hence, the question of remembering and forgetting is not a question that should be decided at a given moment but a question that society should keep open for future generations to decide under their respective circumstances. Consequently, the legal concept of responsibility calls for a *duty to sustainably preserve the freedom of action for future generations*. At the same time, preserving information for future uses comes with a responsibility for future users who need to learn how to handle information about the past. To avoid the feared restrictions that individuals may feel when they know that information about their present will still be available in the future (Sigrist, 2014; Richards, 2013; Solove, 2007; Askin, 1972). Future users will need to learn that information about the past – although still useful today – relates to the past and must not be used to restrict individuals' ability to change their behaviour in the future.

With regard to the precautionary approach and the preservation of freedom of action, we argue that the guiding principle of this design guide must be that the storage of data is not only today's technological default but that remembering information should also be enabled and encouraged both by legislators and rule-makers within private and public organisations.

Hierarchy of concepts

Applying a precautionary approach means that deleting information cannot be the default solution. Instead, given the uncertainty of possible future uses of information, the default must be that information about the past will be stored so that future generations can have access to it if they deem that information useful. As a consequence, we strongly advocate for the recognition of a hierarchy of concepts. According to this hierarchy, deleting information is the ultimate solution and should only take place if no alternative mechanisms such as access restrictions, use restrictions or the transfer of data can be applied (for these alternative mechanisms see below, 3b). The aim of this hierarchy of mechanisms is to ensure that remembering can be established and sustainably upheld as the default solution of the digital age. This new default, however, can only be successfully established in a legal system, if the interests that might advocate for deleting information can be sufficiently protected on a case-by-case basis, e.g. by restricting the access or use of the respective set of information.

Process, not rules

The comprehensive scope of application, the complexity of the problem and the existing uncertainty at the technological and societal level make establishing specific, substantive rules for remembering and forgetting of information an overly difficult, if not impossible, task. Instead of providing such substantive rules, this design guide therefore recommends to establish a process that consists of possible alternatives to deleting information and of a set of criteria that must be considered when deciding whether information should be remembered or forgotten. Given the uncertainty of future developments in technology, society and law, the framework proposed in this design guide is not necessarily able to withstand the test of time. Therefore, the framework itself needs to leave room for change and will have to be revised periodically and adapted to new environments if necessary.

Policy considerations

Regulatory approach

According to the precautionary approach, current trends that advocate for a default of deleting information must be mitigated, by emphasising the fundamental societal need to remember. Looking at the efficacy of regulation, however, any policy proposal seeking to tip the balance back towards a default of remembering, needs to be flexible enough to be adapted to the specific needs of the respective organisation which may change over time. Although these requirements clearly raise the bar for effective and efficient regulation, they do not substantively differ from the standards that existing data protection regulations must meet. Consequently, we believe that the framework proposed in this design guide can be implemented without altering established principles of data protection law.

A fundamental distinction of many data protection laws is the distinction between public and private entities. While substantive standards do not much differ, the regulatory approach is different. Public entities are subject to direct regulation (so-called command and control regulation), which implements the requirement of a sufficient legal basis as a core requirement for the handling of personally identifiable data. Private entities are subject to a mixed approach: Their handling of personally identifiable data is mostly based on the unilateral consent of the individuals concerned or on a bilateral and therefore contractual consensus between the affected parties, but it may also be the consequence of prevailing public or private interests that justify the handling of such data. In any case, the law provides private and public entities with a great deal of discretion when handling personally identifiable data. Looking at the complexity of remembering and forgetting, such leeway seems to be even more justified when adding the additional layers of scrutiny contained in the design guide. Command and control regulation, in this context, might be inflexible, inefficient and may well prove to be ineffective as well.

As a result of the vast amount of data, the responsibility for compliance lies with the entity handling the data. To enforce existing standards, current data protection law relies on a portfolio of public and private agents (supervisory authorities, certification procedures, self-assessment, reporting). This setting to ensure compliance does not need to be changed.

Policy proposals

As mentioned above, implementing a due process for remembering and forgetting constitutes a burden in terms of cost and personnel on any entity. Without any incentives, public and private entities may choose to avoid the burdens of the process set out in the design guide. However, compliance with the process might be improved by setting a new or altering the existing *incentive structure*, rather than just relying on mandatory legal provisions. Requiring reporting and setting up benchmarking procedures (*naming and shaming*), by providing technical assistance or financial support (subsidies) may set such incentives, inter

alia, by granting adequate tax relief or by establishing rules of best practices and self-regulatory bodies.

Incentives to implement effective procedures for decision-making may also counteract tendencies of power concentration, meaning that only larger archival structures might achieve reliable long-term memories. However, cultural, societal and economical needs for remembering may be better served by having memory distributed in several, probably even redundant archival structures, which may be controlled by both public and private actors. Private archives, in particular smaller archives, might struggle to comply with the process set out in the design guide. To circumvent such struggles and to award their efforts, these archives will most probably need some kind of support. Such support seems to be a *conditio sine qua non* to establish successfully a *power balance* between public archives, private archives of powerful business organisations such as multinational enterprises and private archives focussing on the data of small and medium sized enterprises and individuals.

Although the framework of this design guide can be implemented without changing established data protection principles, the application of some of these principles will need to be readjusted. For example, when assessing the legitimacy of storing personally identifiable data by balancing the interests of the data controller and data subjects, societies' interest in remembering should always be taken into account. At least if personally identifiable data is stored in a private or public archive with adequate and duly implemented access restrictions, societies' need to remember should generally prevail. Furthermore, copyright law may need to be amended by implementing a new limitation that allows archives to make and store copies of subject matter that is protected by a copyright or a related right, including the sui generis right for the protection of databases.

Framework

Process

The framework aims at providing a process that those responsible for setting the rules for handling information should go through when regulating the remembering and forgetting of information. This process should be applied both by international, national and regional legislators as well as by those setting the rules for information handling in public and private organisations. Although this process cannot relieve legislators and other rule-makers from their duty to make a decision, its application is meant to ensure better informed and more deliberate decisions when regulating remembering and forgetting. In addition, this process can be directly implemented in private organisations if the people responsible for the information management are granted sufficient discretion for applying its rather abstract criteria. In this case, the process will have to be applied every time a decision on remembering or forgetting must be made.

The process consist of two blocks that must be considered when taking this decision.

1. A number of *alternative mechanisms* that can be applied instead of forgetting information by consciously deleting it.
2. A set of *criteria* (see for similar criteria catalogues with regard to the *Right to be Forgotten*: Court of Justice of the European Union. Article 29 Data Protection Working Party, 2014; Google Corporation. The Advisory Council to Google on the Right to be Forgotten, 2015).

To ensure transparency and accountability for current and future generations, the application of this decision-making process must always be sufficiently documented and recorded. For the application of the process, it is important to note that the two blocks are not different steps within the decision-making process. Rather, they are interdependent, i.e. the decision to delete eventually information must always consider alternative mechanisms that allow for the sufficient protection of the interests that may advocate

for deleting. As a result, deleting should only take place if the criteria applied call for this ultimate step and if no alternative mechanism is available.

(1) Alternative mechanisms	(2) Criteria
a. access restrictions	a. relevance of information
b. use restrictions	b. impact of information
c.transfer of data	c. redundancy of information
	d. efficacy of deleting

In most cases, the application of this process will lead to the conclusion that the information should not be deleted. This conclusion may be supported by the absence of a serious impact on specific individuals, the interests of society, the possible relevance of the information for future generations and the availability of alternative mechanisms. However, in case specific information has a heavy impact on one or more individual(s), such as discriminatory effect, the potential lack of relevance for others including future generations and the limited protection that access and use restrictions can afford, the deletion of the respective information may be the adequate solution.

The deliberate decision to remember specific information has two major consequences: first, the individual or organisation in possession of the information must make sure that the information is constantly migrated from the current to the next generation of technology. Second, the individual or organisation must ensure that the process described above is reapplied at a later point in time since the decision to remember information is always time-dependent and must therefore be *reviewed periodically*. The length of the period for reviewing the decision depends on the lifecycle of the storage technology, the respective information and the individual or organisation and should be defined ex ante either by the legislator or by those setting the rules for information handling within an organisation, possibly accompanied by default rules set by the legislator. Furthermore, a need to review the decision may be triggered by internal or external events such as a company reaching the size for mandatory auditing or listing the company at a stock exchange.

In addition to the need to review decisions on remembering and forgetting, the *decision-making process* itself will have to be reviewed from time to time since the criteria and the alternative mechanisms are in themselves, like information, in no way independent of time. From this perspective, the decision-making process must be seen as a flexible framework that has to be re-evaluated from time to time. To ensure a meaningful re-evaluation, rule-makers should try to establish a feedback-loop, i.e. a mechanism that provides information on the acceptance of decisions taken by applying the decision-making process. Sunset regulation may help to evaluate the decision-making process.

Alternative mechanisms

Access restrictions. From the perspective of individuals and organisations affected by the existence and availability of information, restricting the access to such information can provide similar effects as deleting it does. The most prominent example for this widely applied mechanism are national archives that preserve vast amounts of information thereby restricting the access for the general public until the term of protection, usually 50 years for personally identifiable data, has lapsed. Access restrictions often present a viable and valuable alternative to deleting information since such restrictions enable the balancing of interests between individuals or organisations that might be negatively affected by the current availability of the information and the interests of future generations in preserving the information

for their possible future uses.

Use restrictions. More often than not, individuals and organisations are not negatively affected by the mere existence and availability of information but rather by the specific use of such information. In such cases, both deleting the information and restricting the access would be unnecessarily invasive. Instead, the interests of individuals and organisations can be sufficiently protected by restricting certain uses all the while preserving the information for possible future uses.

Transfer of data. Instead of establishing access restrictions, the information holder might transfer the respective data to a third party – namely to a public or a private archive – that serves as a trusted institution and already has established alternative mechanisms such as access restrictions. In our view, the transfer of data to an archive should become the default solution not only for government agencies – as existing legislation – but also for private organisations and individuals. For the latter, the transfer of data to an archive should at least take place when the organisation ceases to exist, e.g. because of going out of business, or when an individual dies.

Criteria

Relevance of information. This criterion calls for the assessment of the relevance of information in a very broad sense, including its potential relevance for the future. Therefore and somewhat opposed to established data protection principles, the relevance of data is neither connected to nor limited to the initial purpose of its collection in a way that calls for deleting the data once this purpose has been fulfilled. Instead, and above all, the assessment must take possible future uses into account that may be completely different from the purpose for which the data were initially collected. When assessing the relevance, a number of factors should be considered, including but not limited to the nature of the information (e.g. information relevant for political discourse, criminal activity, or other topics of public interest), the source (e.g. a world-renowned newspaper or a private diary), the accuracy and the age of data (e.g. health data stemming from the youth of a potential employee vs. data regarding his/her current condition) as well as the (public) role of the individual or organisation concerned.

Impact. This criterion takes the impact of the existence and/or availability of information on the individual or organisation concerned into account and aims at determining how the individual is affected by the further storage or the deletion of the information. The potential impact depends on a number of factors, including, but not limited to, the sensitivity of the data, potential discriminatory effects, the risk of misuse of the data and the power of the information holder to distribute and/or use such data. As opposed to the criterion of relevance, the criterion of impact focusses on the individual or the organisation concerned rather than on the interests of third parties or the society. Accordingly, the individual or organisation concerned may need to be involved in the decision-making process to ensure that all relevant factors are taken into account when assessing the impact of the data.

Redundancy of information. When deciding whether to retain or to delete data, the fact that such data is available from other sources is a key element that needs to be considered. If the data is available from another source, deleting such data seems to be relatively unproblematic. However, the precautionary approach and the intended power balance may call for storing such data despite the fact that it is available elsewhere. In addition, redundant storing may be important where a specific information holder is able to restore the context of a specific piece of information while other information holders cannot.

Efficacy of deletion. An additional criterion that needs to be considered is whether the information can be deleted effectively to fulfil the intended purpose of excluding all and any future uses. If one cannot ensure that the information will not be accessible, retrievable and readable after the deletion, the information holder should consider storing such information until effective deletion can be carried out.

Final Observations

With regard to the framework and the main observations of the research project, three final observations must be made.

Trust in change

Acknowledging the importance of time in the decisions on information handling also implies the acknowledgement of time in decisions on the acknowledgment of time (so called meta-acknowledgement).

This meta-acknowledgement requires that, irrespective of the procedures that are set in place and the criteria on the timeliness of the information, they have to recognise and ascertain that such processes and criteria remain open and reversible in time (see above, 2c). This is the fundamental decision for freedom in the way information societies handle their information. It also implies that trust in the future development of the way we handle information is assumed.

While, for example, some national constitutions seek to safeguard the inner workings of their society and fundamental rights by declaring that their constitutions are, at least in parts, non-alterable, other legal systems put their trust into the representative institutions of the people, their insights, their intentions and their abilities to maintain essential values. It is in this spirit of trust that we assume that the process of deciding on what is remembered and what is forgotten can remain open to future changes.

Importance of context

With the recognition of timeliness and the importance of time, we also acknowledge the immense importance of context in information handling.

From a time perspective, recognising the importance of context is not just about the relation between different pieces of information but also about the ability to base decisions for the future on information from and about the past, thereby guaranteeing a certain level of historic awareness.

In our view, the dimension of time can best be seen as an ingredient of the contextual character of information. Decisions based on information that we evaluate as being incomplete, unjust, or unfair imply negligence in the way context is being treated. We do hope that by putting emphasis on the time dimension of information handling, we have also contributed to the understanding how necessary the context of information is for future decision-making processes.

From this perspective, promoting the importance of remembering can also be seen as an important means to ensure the re-establishment of context in the future. Given today and future information retrieval and recombination technologies, storing vast amounts of data, preferably at various sources, should allow for the re-establishment of context if needed.

Conflict with existing data protection principles

The aim of both accepting and fostering remembering as the information handling default of the digital age is not free from conflict with current data protection principles. The broad discretion that comes with the very open notion of principles such as fair and lawful processing, purpose limitation and proportionality, however, should allow resolving these conflicts to a certain extent when applying data protection law. Yet, according to the principle of purpose limitation the preservation of information for future uses may only be acceptable in certain cases if the person concerned gives his/her consent. Despite

this positive assessment, the concept of remembering as a default directly contradicts the established principle of data minimisation (European Union, 1995, Art. 6 (c) Data Protection Directive; more explicitly: European Union, 2012, Art. 5 (c) Draft General Data Protection Regulation). At the beginning of designing an information handling process, this principle raises the question whether the data to be collected is necessary for the intended purposes or whether there are procedures that require the use of less personally identifiable information while achieving the same goal. Even more importantly, once the data has been collected, the principle of data minimisation requires that personally identifiable data are stored for the shortest time possible. According to recital 30 Draft General Data Protection: 'the period for which the data are stored must be limited to a strict minimum' and 'time limits should be established by the data controller for erasure of the data or for a periodic review'.

We note that this is not a must-have principle in the current legal system but a *consideration* that should be taken into account in the interest of privacy. However, the principle of data minimisation contains a critical evaluation with regard to information holdings: it precludes the result of a comprehensive cost-benefit analysis assuming that the potential harm of collecting information is higher than the potential benefit. It must be noted that it is precisely this type of decision-making that excludes the proper realisation of the time dimension of information handling, namely, that applications of that information may be possible in the future, which would create more benefits than costs. By ignoring possible future benefits and focussing on potential harms in the present, the principle of data minimisation precludes a cost-benefit analysis that can only be fully made in the future.

Furthermore, the data minimisation principle also contains a pre-judgment on the possibilities to control information in the future. In this respect, it expresses a fundamental distrust that decisions in the future will not respect decisions made in the present. It is – so to speak – an attack of the present on the future and expresses a fundamental distrust in the solidity of our institutions, their functions and their values in the future. Proclaiming such an assumption in our opinion is not just a statement of personal preferences and values. It is both an exclusion of possible better controls and higher benefits of information handling in the future, and includes a negative judgment on the developments of information technology and its legal frameworks in the past and in the present.

We do not share this attitude and we do not think that this is an act of belief. We hold instead that both legislators and rule-makers in private and public organisations of the present have – as in other areas – a responsibility with regard to the future for what they regulate today and that the openness this entails is to be clearly preferred to closing the future.

Conclusion

This position paper aims at counterbalancing a recent trend in privacy literature that advocates for establishing mechanisms of automated deletion of (personally identifiable) information to protect privacy. In our view, favouring deletion over storage and forgetting over remembering is a rather shortsighted reaction to the storage of vast amounts of data, which is one of the key characteristics of the digital age. Instead of establishing deletion as the new default and thereby inhibiting possible future uses of information, we propose to decide on the remembering and forgetting of information by applying a balanced decision-making process. This process consists of (1) alternative mechanisms to deletion such as access restrictions, use restrictions and the transfer of data to trusted institutions such as public or private archives and (2) a set of criteria to decide on remembering or forgetting, namely the relevance, impact and redundancy of information and the efficacy of deletion. In our view, the application of this process should foster the preservation of information for future generations while adequately protecting the interests of the individuals concerned.

Acknowledgements

This position paper is one of the results of the project *Remembering and Forgetting in the Digital Age* funded by the Swiss National Science Foundation (grant no. 10001A-140887) and jointly carried out by the Research Center for Information Law, University of St.Gallen and the Berkman Center for Internet and Society, Harvard Law School. We are grateful to Prof. Dr. Urs Gasser, Executive Director of the Berkman Center for Internet and Society, who supported this project at every research step over the past three years.

About the authors

Florent Thouvenin is Assistant Professor (tenure track) for Information and Communication Law, Center for Information Technology, Society, and Law, University of Zurich, Rämistrasse 74/49, 8001 Zürich, Switzerland. Florent Thouvenin holds the newly founded chair of Information and Communications Law at the University of Zurich. His research focuses on intellectual property and information law with an emphasis on copyright and data protection law. He can be contacted at florent.thouvenin@rwi.uzh.ch
Herbert Burkert is Professor Emeritus for Public Law with special focus on Information and Communication Law, Research Center for Information Law, University of St.Gallen, Bodanstrasse 6, 9000 St.Gallen, Switzerland. herbert.burkert@unisg.ch. Herbert Burkert's research focuses on information and communication law, including issues of constitutional law. His e-mail address is herbert.burkert@unisg.ch
Peter Hettich is Professor for Public Business Law, Institute of Public Finance, Fiscal Law, and Law and Economics, University of St.Gallen, Varnbüelstrasse 16, 9000 St. Gallen, Switzerland. peter.hettich@unisg.ch. His main research interests lie in the fields of economic and social regulation of enterprises, risk regulation and antitrust. He can be contacted at peter.hettich@unisg.ch
Rehana Harasgama is PhD Candidate at the Research Center for Information Law, University of St.Gallen, Bodanstrasse 6, 9000 St. Gallen, Switzerland. Rehana Harasgama studied law at the University of St.Gallen and worked as a research assistant for the FIR-HSG. In her internship at a big accounting firm in Zurich, Rehana is currently acting as the internal data protection officer for Switzerland. Her e-mail address is rehana.harasgama@unisg.ch

References

- Askin, F. (1972). Surveillance: the social science perspective. *Columbia Human Rights Law Review, 4,* 59-88.
- Beglinger, J., Burgwinkel, D., Lehmann, B., Neuenschwander, P. & Wildhaber, B. (2008). *Records Management: Leitfaden zur Compliance bei der Aufbewahrung von elektronischen Dokumenten in Wirtschaft und Verwaltung mit Checklisten, Mustern und Vorlagen [Records Management: Handbook for Compliance when Storing Electronic Documents in Industry, Commerce, and Administration with Checklists, Models and Templates]* (2nd. ed.). Zollikon, Switzerland: Kompetenzzentrum Records Management GmbH.
- Court of Justice of the European Union. Article 29 Data Protection Working Party (2014). *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* (C-131/12), 14/EN WP 225. Retrieved from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (Archived by WebCite® at http://www.webcitation.org/6dwS8Ws4u).
- Digital Rights Ireland Ltd vs. Minister for Communications, Marine and National Resources et al. (2014). European Court of Justice, 8 April 2014, C-293/12 and C-594/12.
- European Union (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).
- European Union (2002). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).
- European Union (2012). Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Draft General Data Protection Regulation), 25 January 2012, COM/2012/011 final.
- Google Spain SL et al. vs. Mario Costeja Gonzalez et al. (2014). European Court of Justice, 13 May 2014, C-131/12.
- Google Corporation. The Advisory Council to Google on the Right to be Forgotten (2015). *The report of the Advisory Committee to Google on the Right to be Forgotten.* Retrieved 15 April 2015 from https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pli=1 (Archived by WebCite® at http://www.webcitation.org/6eMRQGUqj)
- Harvey, R. (2010). *Digital curation, a how-to-do-it manual.* New York: Neal-Schumann Publishers.
- Mayer-Schönberger, V. (2009). *Delete: the virtue of forgetting in the digital age.* Princeton, New Jersey: Princeton University Press.
- Richards, N. M. (2013). The dangers of surveillance. *Harvard Law Review, 126*, 1934-1965.
- Schwartz, P. & Solove, D. (2011). The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review, 86*, 1814-1894. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366 (Archived by WebCite® at http://www.webcitation.org/6dwSTTDQO)
- Sigrist, M. (2014). *Staatsschutz oder Datenschutz? Die Vereinbarkeit präventiver Datenbearbeitung zur Wahrung der inneren Sicherheit mit dem Grundrecht auf informationelle Selbstbestimmung [State security or data protection? The compatibility of preventative data processing for the safeguarding of internal security with the fundamental right to informational self-determination].* Zurich, Switzerland: Schulthess.
- Solove, D. (2007). I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review, 44*, 745-772. Retrieved from http://papers.ssrn.com

How to cite this paper

Thouvenin, F., Burkert, H., Hettich, P. and Harasgama, R. (2016). Remembering and forgetting in the digital age – a position paper. *Information Research, 21*(1), paper memo2. Retrieved from http://InformationR.net/ir/21-1/memo/memo2.html (Archived by WebCite® at http://www.webcitation.org/6gArDmqol)

- Contents |
- Author index |
- Subject index |
- Search |
- Home